PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07C 15/00, G06F 1/00 — A1

(11) Numéro de publication internationale: **WO 96/34368**

(43) Date de publication internationale: 31 octobre 1996 (31.10.96)

(21) Numéro de la demande internationale: PCT/FR96/00645

(22) Date de dépôt international: 26 avril 1996 (26.04.96)

(30) Données relatives à la priorité:
95/05175 28 avril 1995 (28.04.95) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: INFO TELECOM [FR/FR]; Rue de la Forêt, F-67550 Vendenheim (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(US seulement)*: BERNHARD, François [FR/FR]; 55, rue de Mulhouse, F-67100 Strasbourg (FR). BREMAUD, Patrice [FR/FR]; 26, rue du Général-Leclerc, F-67550 Vendenheim (FR).

(74) Mandataire: BUREAU D.A. CASALONGA JOSSE; 8, avenue Percier, F-75008 Paris (FR).

(81) Etats désignés: AU, BR, CA, CN, JP, MX, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée

Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: TAMPER PROTECTION AND ACTIVATION METHOD FOR AN ELECTRONIC GAMING DEVICE AND DEVICE THEREFOR

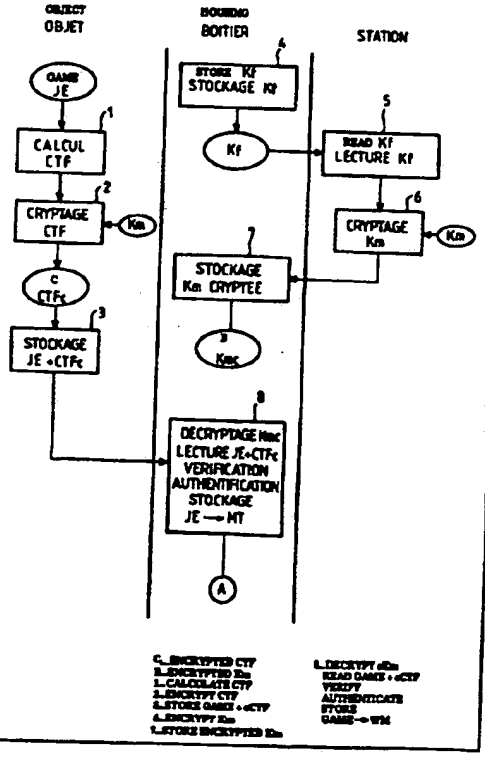
(54) Titre: PROCEDE D'ACTIVATION ET DE PROTECTION ANTI-FRAUDE D'UN DISPOSITIF ELECTRONIQUE DE JEU, ET DISPOSITIF CORRESPONDANT

(57) Abstract

An electronic gaming device has one or more housings with at least one result-encryption key stored therein, as well as a portable article adapted for co-operating with the housing and with a set of authenticatable digital game data representative of a game stored therein. The portable article is made to co-operate with the housing. The set of game data is authenticated in the housing and stored in a working memory of the housing so as to authorise the progression of the game in the housing. After completion of at least part of the game, result information dependent on said game is encrypted in the housing by means of at least one result-encryption key, and the encrypted result information is stored in a result memory of the portable article, which then co-operates with a validation station capable of accessing the result-encryption key, whereafter said station verifies the result information.

(57) Abrégé

Le dispositif électronique de jeu comporte au moins un boîtier dans lequel a été stockée au moins une clé de cryptage-résultat, ainsi qu'au moins un objet portatif capable de coopérer avec le boîtier et dans lequel a été stocké un ensemble de données numériques de jeu authentifiables et représentatif d'un jeu. On fait coopérer l'objet portatif avec le boîtier. On vérifie au sein du boîtier l'authentification de l'ensemble de données de jeu et on stocke cet ensemble de données de jeu dans une mémoire de travail du boîtier, de façon à autoriser le déroulement du jeu au niveau du boîtier. Puis, après le déroulement d'au moins une partie du jeu, on crypte au sein du boîtier une information de résultat dépendante dudit jeu à l'aide au moins de ladite clé de cryptage-résultat, et on stocke cette information de résultat cryptée dans une mémoire de résultat de l'objet portatif. Puis, on fait coopérer l'objet portatif avec une station de validation ayant accès à ladite clé de cryptage-résultat, ladite station vérifiant ladite information de résultat.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AM	Arménie
AT	Autriche
AU	Australie
BB	Barbade
BE	Belgique
BF	Burkina Faso
BG	Bulgarie
BJ	Bénin
BR	Brésil
BY	Bélarus
CA	Canada
CF	République centrafricaine
CG	Congo
CH	Suisse
CI	Côte d'Ivoire
CM	Cameroun
CN	Chine
CS	Tchécoslovaquie
CZ	République tchèque
DE	Allemagne
DK	Danemark
EE	Estonie
ES	Espagne
FI	Finlande
FR	France
GA	Gabon
GB	Royaume-Uni
GE	Géorgie
GN	Guinée
GR	Grèce
HU	Hongrie
IE	Irlande
IT	Italie
JP	Japon
KE	Kenya
KG	Kirghizistan
KP	République populaire démocratique de Corée
KR	République de Corée
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Libéria
LT	Lituanie
LU	Luxembourg
LV	Lettonie
MC	Monaco
MD	République de Moldova
MG	Madagascar
ML	Mali
MN	Mongolie
MR	Mauritanie
MW	Malawi
MX	Mexique
NE	Niger
NL	Pays-Bas
NO	Norvège
NZ	Nouvelle-Zélande
PL	Pologne
PT	Portugal
RO	Roumanie
RU	Fédération de Russie
SD	Soudan
SE	Suède
SG	Singapour
SI	Slovénie
SK	Slovaquie
SN	Sénégal
SZ	Swaziland
TD	Tchad
TG	Togo
TJ	Tadjikistan
TT	Trinité-et-Tobago
UA	Ukraine
UG	Ouganda
US	Etats-Unis d'Amérique
UZ	Ouzbékistan
VN	Viet Nam

Procédé d'activation et de protection anti-fraude d'un dispositif électronique de jeu, et dispositif correspondant.

L'invention concerne l'activation et la protection anti-fraude d'un dispositif électronique de jeu et le dispositif correspondant.

On connaît actuellement différents jeux, notamment des jeux de hasard, permettant à un joueur de gagner des sommes d'argent moyennant le paiement d'une mise de départ. Ainsi, par exemple dans le jeu appelé "Loto" (marque déposée) le joueur coche une série de chiffres sur un ticket qu'il fait valider auprès d'un organisme spécialisé en acquittant un prix correspondant à la mise de départ. Un tirage au sort ultérieur est effectué sous contrôle dans un endroit choisi et, les joueurs en possession d'un ticket gagnant peuvent retirer leurs gains auprès d'un organisme payeur.

D'autres jeux consistent à se procurer un ticket et à gratter celui-ci en des endroits désignés de façon à découvrir des informations permettant de définir si le ticket en question est gagnant ou perdant.

Par rapport à ces jeux classiques nécessitant un support-papier, il a déjà été envisagé de proposer, dans le brevet français n° 92 13 239, un concept radicalement différent de dispositif de jeu de hasard.

Selon ce concept, il est prévu un boîtier portable destiné à permettre à un joueur d'effectuer une ou plusieurs épreuves de jeux de hasard, la réussite ou l'échec auxdites épreuves conditionnant un score ou un niveau de gain suivant des règles de jeu prédéterminées. Ce boîtier constitue alors également l'élément de transaction pour le paiement du gain et comporte tous les éléments nécessaires pour la vérification de celui-ci.

Cependant, de par sa conception et notamment pour des raisons de sécurité, chaque boîtier autonome ne peut être utilisé qu'une seule et unique fois. Ceci pose naturellement un problème économique et écologique en raison de cette utilisation unitaire combinée avec une diffusion estimée de l'ordre de plusieurs dizaines de millions d'unités par mois.

Outre le fait que ce type de boîtier ne peut être utilisé qu'une seule fois, il est par ailleurs associé à un type de jeu unique. Or, le marché actuel des jeux de hasard montre que la durée de vie d'un type de jeu est généralement courte et que ceux-ci doivent être renouvelés souvent ce qui conduit alors le fabricant du boîtier à concevoir en permanence de nouvelles formes extérieures pour le produit ainsi que de nouvelles interfaces logicielles.

L'invention vise à apporter une solution à ces problèmes.

Un but de l'invention est de proposer un dispositif électronique de jeu capable d'être utilisable plusieurs fois avec éventuellement différents types de jeu.

Un problème très important inhérent à de tels dispositifs de jeu réside dans la sécurité anti-fraude, en particulier lorsque certains types de jeu sont associés à des gains importants.

L'invention vise par conséquent à intégrer cette notion de sécurité dans un dispositif de jeu multi-applications et multi-utilisations.

L'invention propose donc tout d'abord un procédé d'activation et de protection anti-fraude d'un dispositif électronique de jeu comportant au moins un boîtier dans lequel a été stocké au moins une clé de cryptage-résultat, ainsi qu'au moins un objet portatif capable de coopérer avec le boîtier, et dans lequel a été stocké un ensemble de données numériques de jeu authentifiable et représentatif d'un jeu. Selon ce procédé, on fait coopérer l'objet portatif avec le boîtier. On vérifie au sein du boîtier l'authentification de l'ensemble de données de jeu et on stocke cet ensemble de données de jeu dans une mémoire de travail du boîtier, de façon à autoriser le déroulement du jeu au niveau du boîtier. Puis, après le déroulement d'au moins une partie du jeu, on crypte au sein du boîtier une information de résultat

dépendante dudit jeu, à l'aide au moins de ladite clé de cryptage-résultat. On stocke cette information de résultat cryptée dans une mémoire de résultat de l'objet portatif. Puis, on fait coopérer l'objet portatif avec une station de validation ayant accès à ladite clé de cryptage-résultat, ladite station effectuant un traitement de validation à partir au moins de ladite information de résultat cryptée et de ladite clé de cryptage-résultat.

Ainsi, selon l'invention, on déporte les données numériques de jeu, c'est-à-dire l'applicatif ou le logiciel de jeu, à l'extérieur du boîtier électronique et on l'incorpore dans une mémoire d'un objet portatif qui peut se présenter sous différentes formes, telles que carte de crédit, domino, jeton, etc.

Quant au boîtier électronique, celui-ci peut être vendu une seule fois et être utilisable plusieurs fois avec tout objet portatif contenant un logiciel de jeu.

Selon l'invention c'est donc l'objet portatif qui est destiné à contenir à la fois les données numériques de jeu définissant le jeu proprement dit, ainsi que l'information de résultat permettant au joueur de faire valider ce résultat de façon à toucher éventuellement son gain. En d'autres termes, l'objet portatif constitue ici l'élément de transaction tandis que le boîtier ne sert uniquement au joueur que pour jouer.

La notion de "cryptage" doit s'interpréter très largement comme étant une "protection à l'aide de moyens cryptographiques". Ceci étant, à des fins de simplification, seuls les termes cryptage, décryptage, crypter, décrypter seront employés dans la suite du texte.

L'information de résultat qui va être cryptée dans le boîtier avant d'être transférée dans l'objet portatif, dépend naturellement de la nature du jeu. Il peut s'agir par exemple d'une information binaire du type "gagné" ou "perdu", ou bien encore, par exemple, d'une information représentative d'un niveau de gain.

Pour des raisons de sécurité, l'ensemble de données numériques de jeu stocké dans l'objet portatif est authentifiable de façon à permettre la vérification de son authentification au sein du boîtier. Au sens de la présente invention, le mot "authentifiable" doit

être interprété de façon large incluant par exemple un stockage en "clair" des données numériques de jeu proprement dites conjointement à un certificat d'authentification obtenu, à partir de ces données numériques de jeu, par un algorithme approprié, ou bien encore un cryptage au moins partiel de cet ensemble, ou par exemple un cryptage du certificat d'authentification.

La vérification de l'authentification de l'ensemble de données de jeu peut s'effectuer avant, pendant ou après le stockage de celui-ci dans la mémoire de travail du boîtier.

Il convient également de remarquer ici que, selon l'invention, l'ensemble des données numériques de jeu est transféré dans la mémoire de travail du boîtier (en pratique ces données sont par exemple lues dans l'objet portatif puis recopiées dans la mémoire de travail du boîtier) de sorte que la coopération entre l'objet portatif et le boîtier pourrait éventuellement être supprimée pendant le déroulement du jeu au niveau du boîtier.

L'invention évite donc ainsi l'emploi de moyens logiciels complexes que nécessiterait l'exploitation directe du logiciel de jeu de l'objet portatif par l'unité de traitement du boîtier sans transfert dans la mémoire du boîtier. Aussi, selon un mode de mise en oeuvre du procédé selon l'invention, il est avantageusement prévu que l'ensemble de données de jeu d'un objet portatif soit lu par l'intermédiaire d'un protocole série entre l'objet portatif et le boîtier. Ce qui permet de minimiser les moyens matériels et logiciels de l'objet portatif. L'exploitation directe du logiciel de jeu s'effectue par l'unité de traitement du boîtier directement dans la mémoire de travail de celui-ci.

D'une façon très générale, le traitement de validation effectué par la station de validation doit permettre de déterminer et/ou de vérifier l'information de résultat à partir du contenu de l'objet portatif. En effet seul ce contenu mémorisé doit faire foi pour autoriser un paiement éventuel d'un gain.

Le traitement de validation effectué par la station de validation peut comporter un décryptage de l'information de résultat cryptée et stockée dans la mémoire de résultat de l'objet portatif, à

l'aide de la clé de cryptage-résultat.

En variante, ce traitement de validation peut s'effectuer d'une manière différente. Plus précisément, on peut stocker dans l'objet portatif, conjointement avec l'information de résultat cryptée, l'information de résultat non cryptée c'est-à-dire "en clair". La station vérifie alors ladite information de résultat en recryptant, à l'aide de la clé de cryptage-résultat, l'information de résultat non cryptée qui est stockée dans l'objet portatif et en comparant cette information de résultat recryptée avec l'information de résultat cryptée et stockée dans la mémoire de résultat de l'objet portatif.

Afin d'augmenter encore la sécurité, il est avantageusement prévu que lorsque l'authentification de l'ensemble de données de jeu de l'objet portatif a été vérifié et que ledit ensemble a été stocké dans la mémoire du travail du boîtier, on interdise toute exploitation ultérieure par le boîtier, de l'ensemble de données de jeu de cet objet portatif.

Ceci permet notamment d'éviter qu'un joueur ne s'entraîne à jouer à un type de jeu, en particulier lorsque celui-ci est en fait un jeu de réflexe.

Au sens de la présente invention, l'interdiction de toute exploitation ultérieure doit s'entendre dans un sens très large signifiant par exemple que, soit le boîtier ne peut plus lire l'ensemble de données, soit il ne peut plus vérifier son authentification. En d'autres termes, le boîtier sera alors inapte au jeu avec cet objet portatif.

Le dispositif selon l'invention comprend généralement plusieurs boîtiers et plusieurs objets portatifs. Aussi, lorsque l'authentification de l'ensemble de données de jeu de l'un des objets portatifs a été vérifiée et que ledit ensemble a été stocké dans la mémoire de travail de l'un des boîtiers, on interdit alors avantageusement toute exploitation ultérieure par l'un quelconque des boîtiers, de l'ensemble de données de jeu de cet objet portatif.

Selon un mode de mise en oeuvre du procédé selon l'invention, on peut authentifier l'ensemble de données de jeu stocké dans l'objet portatif en y adjoignant un certificat d'authentification lié

de façon biunivoque aux données numériques de jeu. La vérification de l'authentification de l'ensemble de données de jeu comporte alors un recalcul du certificat d'authentification au sein du boîtier et une comparaison entre le certificat d'authentification recalculé et le certificat d'authentification stocké dans l'objet portatif.

Ainsi, on peut interdire toute exploitation ultérieure d'un ensemble de données de jeu en altérant dans l'objet portatif correspondant, au moins partiellement ledit certificat d'authentification et/ou au moins partiellement les données de jeu proprement dites. On peut à cet effet envisager de modifier arbitrairement la valeur de certains des bits du certificat d'authentification et/ou de certaines des données numériques de jeu. De ce fait, si un joueur essaye de rejouer avec le même objet portatif, l'unité de traitement du boîtier recalculera un certificat d'authentification qui diffèrera du certificat d'authentification altéré, ce qui interdira toute activation du jeu.

Toujours dans le but d'augmenter la sécurité, notamment en ce qui concerne le paiement de gains éventuels, on autorise avantageusement le stockage de l'information de résultat cryptée dans l'objet portatif que si l'on a, au préalable, interdit toute exploitation ultérieure de l'ensemble de données de jeu de cet objet portatif.

Selon un mode de mise en oeuvre du procédé, on peut stocker dans le boîtier au moins une clé de cryptage-jeu. L'authentification de l'ensemble de données de jeu stocké dans l'objet portatif peut comporter alors un cryptage au moins partiel de cet ensemble de données de jeu, ou d'une information reliée à cet ensemble de données de jeu (par exemple le certificat d'authentification), à l'aide de la clé de cryptage-jeu, et ce, avant lecture par l'unité de traitement du boîtier, de l'ensemble de données de jeu de l'objet portatif. La vérification de l'authentification de l'ensemble de données de jeu comporte alors un décryptage au sein du boîtier à l'aide de la clé de cryptage-jeu. En d'autres termes, le transfert crypté de l'applicatif, ou du certificat d'authentification associé, permet d'éviter le chargement d'un applicatif frauduleux conduisant inéluctablement à l'obtention d'un gain.

On peut éventuellement ne crypter et ne décrypter que le certificat d'authentification.

Lorsqu'une clé de cryptage-boîtier est stockée dans le boîtier, on peut stocker dans le boîtier la clé de cryptage-jeu qui a été au préalable cryptée à l'aide de la clé de cryptage-boîtier. Ceci permet encore d'augmenter la sécurité et de rendre encore plus difficile la connaissance par un tiers de la clé de cryptage-jeu.

La clé de cryptage-jeu peut être commune à tous les boîtiers et à tous les objets portatifs. La clé de cryptage-boîtier est quant à elle de préférence différente pour chaque boîtier. La clé de cryptage-boîtier d'un boîtier est stockée dans celui-ci avant le stockage de la clé de cryptage-jeu, par exemple lors de sa fabrication. Par ailleurs, l'ensemble de données de jeu d'un objet portatif peut être stocké dans celui-ci, déjà au moins partiellement crypté, ou associé à une information déjà au moins partiellement cryptée, à l'aide de la clé de cryptage-jeu. En d'autres termes, lors de la fabrication en usine des objets portatifs, on peut par exemple déterminer in situ le certificat d'authentification correspondant, crypter ce dernier, et stocker dans l'objet portatif, avant diffusion dans le public, les données de jeu proprement dites suivies de leur certificat d'authentification crypté.

D'une façon générale, la clé de cryptage-résultat peut être la clé de cryptage-boîtier, ou bien la clé de cryptage-jeu, ou bien être obtenue à partir d'une combinaison de ces deux clés.

Lorsque la clé de cryptage-résultat est la clé de cryptage-jeu, toute station de validation connaît cette clé de cryptage-jeu puisqu'elle est commune à tous les éléments du dispositif. Ceci étant, lorsque la clé de cryptage-résultat n'est pas connue à l'avance par la station de validation, il est prévu que l'on stocke dans l'objet portatif coopérant avec le boîtier, une information de clé associée de façon biunivoque à ladite clé de cryptage-résultat, la station de validation ayant alors accès à ladite clé de cryptage-résultat en lisant ladite information de clé stockée dans l'objet portatif.

Ainsi, si par exemple la clé de cryptage-résultat est la clé de cryptage-boîtier, il peut être avantageusement prévu d'associer à chaque boîtier un identifiant le définissant de façon unique, et

permettant d'identifier par là même la clé de cryptage-boîtier qui a été stockée dans le boîtier. Une table d'identifiants peut être par exemple stockée de façon protégée dans un ordinateur central auquel sont reliées toutes les stations de validation. L'identifiant du boîtier est alors stocké avec l'information de résultat cryptée dans l'objet portatif. La station de validation ayant alors accès à l'identifiant ainsi qu'à la table de correspondance peut déterminer la clé de cryptage-résultat et décrypter l'information de résultat cryptée.

L'invention a également pour objet un dispositif électronique de jeu. Selon une caractéristique générale de l'invention, ce dispositif électronique de jeu comprend au moins un boîtier, au moins un objet portatif et au moins une station de validation. L'objet portatif comporte une mémoire de jeu contenant un ensemble de données de jeu authentifiable et représentatif d'un jeu, une mémoire de résultat apte à contenir une information de résultat cryptée, une première interface de communication apte à coopérer avec une interface de communication-boîtier, et une deuxième interface de communication apte à communiquer avec une interface de communication-station. Le boîtier comporte une mémoire de clé contenant au moins une clé de cryptage-résultat, une mémoire de travail accessible en écriture et en lecture, et une unité de traitement reliée à ces mémoires ainsi qu'à l'interface de communication-boîtier. L'unité de traitement est capable, lors d'une coopération entre l'interface de communication-boîtier et la première interface de communication de l'objet, de vérifier l'authentification de l'ensemble de données de jeu mémorisé dans l'objet et de stocker ledit ensemble dans la mémoire de travail de façon à permettre le déroulement du jeu au niveau du boîtier. L'unité de traitement du boîtier est également capable de crypter une information de résultat dépendante dudit jeu, à l'aide de la clé de cryptage-résultat, et de communiquer cette information de résultat cryptée à l'interface de communication-boîtier aux fins de son stockage dans la mémoire de résultat de l'objet. La station de validation comporte des moyens aptes à déterminer ladite clé de cryptage-résultat et des moyens de traitement-station aptes à lire l'information de résultat cryptée via l'interface de communication-

station, lors d'une coopération entre l'objet portatif et la station, et à effectuer un traitement de validation à partir au moins de l'information de résultat cryptée et de la clé de cryptage-résultat.

Dans le cas où le dispositif électronique de jeu comprend plusieurs boîtiers, plusieurs objets portatifs et plusieurs stations de validation, l'un quelconque des objets portatif est capable de coopérer avec l'un quelconque des boîtiers et avec l'une quelconque des stations de validation.

Selon un mode de réalisation du dispositif selon l'invention, la première interface de communication de l'objet portatif est une interface série. Par ailleurs, et pour des raisons d'économie, il est possible de prévoir que l'objet portatif ne comporte qu'une seule et même interface de communication capable de coopérer avec l'interface de communication-boîtier ou avec l'interface de communication-station.

Les moyens de traitement-station peuvent comporter des moyens de décryptage-station aptes à décrypter l'information de résultat cryptée aux fins de sa détermination.

En variante, l'unité de traitement du boîtier est apte à communiquer également l'information de résultat non cryptée à l'interface de communication-boîtier aux fins de son stockage dans la mémoire de résultat de l'objet. Les moyens de traitement-station sont alors en outre aptes à lire l'information de résultat non cryptée via l'interface de communication-station. Ils comportent alors des moyens de cryptage-station aptes à crypter ladite information de résultat non cryptée à l'aide de la clé de cryptage-résultat, ainsi que des moyens de comparaison pour comparer l'information de résultat cryptée recalculée, avec l'information de résultat cryptée stockée dans la mémoire de résultat de l'objet portatif. Cette comparaison permet ainsi de vérifier l'information de résultat.

Lorsque l'ensemble de données de jeu authentifiable est associé à un certificat d'authentification, les moyens de vérification de l'authentification de cet ensemble de données de jeu comportent alors de préférence des moyens de calcul de certificat aptes à recalculer ledit certificat d'authentification au sein du boîtier, à partir de

l'ensemble de données de jeu, et des moyens de comparaison apte à comparer le certificat recalculé et le certificat stocké dans la mémoire de jeu de l'objet portatif.

Selon un mode de réalisation du dispositif, il est possible de prévoir des moyens de cryptage apte à crypter au moins partiellement l'ensemble de données de jeu authentifiable, ou une information reliée à cet ensemble de données de jeu (par exemple le certificat d'authentification), à partir d'au moins une clé de cryptage-jeu. La mémoire de clé du boîtier est alors apte à contenir cette clé de cryptage-jeu tandis que les moyens de vérification de l'authentification de l'ensemble de données de jeu comportent des moyens de décryptage reliés à la mémoire de clé. Ces moyens de cryptage peuvent ne crypter que le certificat d'authentification. Ces moyens de cryptage peuvent être incorporés au sein d'une unité de fabrication de façon à délivrer directement un ensemble de données de jeu au moins partiellement crypté ou un certification d'authentification déjà au moins partiellement crypté, qui sera destiné à être stocké tel quel dans l'objet portatif. Cependant, on peut prévoir en variante que les moyens de cryptage soient incorporés à l'objet portatif, notamment lorsque celui-ci comporte un micro-contrôleur contenant de façon logicielle ces moyens de cryptage.

De même, le fait de prévoir un objet portatif "intelligent", c'est-à-dire pourvu d'une unité centrale par exemple, permet également d'incorporer dans l'objet portatif des moyens permettant d'interdire toute exploitation ultérieure d'un ensemble de données de jeu d'un objet portatif après une première exploitation. Ce moyens, qui peuvent être réalisés par exemple de façon logicielle, sont ainsi par exemple aptes à modifier la valeur de certains des bits de l'ensemble de données de jeu ou de son certificat d'authentification.

D'autres avantages et caractéristiques de l'invention apparaîtront à l'examen de modes de mise en oeuvre et de réalisation de l'invention, nullement limitatifs, et des dessins annexés sur lesquels :

- la figure 1 représente très schématiquement l'architecture matérielle d'un objet portatif d'un dispositif selon l'invention,

- la figure 2 représente très schématiquement l'architecture matérielle d'un boîtier du dispositif selon l'invention,

- la figure 3 représente très schématiquement l'architecture matérielle d'une station de validation du dispositif selon l'invention,

- les figures 4a et 4b illustrent schématiquement un mode de mise en oeuvre du procédé selon l'invention, et

- les figures 5 et 6 illustrent deux variantes de mise en oeuvre du procédé selon l'invention.

Le dispositif selon l'invention comporte plusieurs boîtier électroniques autonomes BT, plusieurs objets portatifs OB et plusieurs stations de validation ST.

Tel qu'illustré sur la figure 1, chaque objet portatif OB, par exemple une carte du type carte à puce, un jeton, ou un module, comporte, par exemple au sein d'un ASIC (Application Specific Integrated Circuit) un micro-contrôleur CPU relié par l'intermédiaire d'un bus à une interface d'entrée sortie ESC du type série, à une mémoire de jeu MJ, ainsi qu'à une mémoire de résultat MR, telle qu'un registre.

Comme on le verra plus en détail ci-après, la mémoire de jeu MJ, par exemple une mémoire morte, est destinée à recevoir un ensemble de données numériques de jeu, ou logiciel de jeu, représentatif d'un type particulier de jeu.

Le registre MR est destiné quant à lui à recevoir une information de résultat cryptée provenant du boîtier BT après le déroulement d'au moins une partie du jeu.

L'interface ESC comporte des moyens de coopération avec une interface homologue ESB du boîtier BT (figure 2) et une interface homologue ESS de la station ST (figure 3). Ces moyens de coopération peuvent consister en un connecteur mécanique ou bien en des moyens de couplage capacitif/inductif, ou optique.

Comme illustrée plus particulièrement sur la figure 2, la structure électronique matérielle du boîtier portable BT s'articule autour d'une unité de traitement UT, telle qu'un microprocesseur ou un micro-contrôleur. Cette unité de traitement UT est reliée par l'intermédiaire d'un bus à une mémoire de travail MT, accessible en

écriture et en lecture, par exemple une mémoire à accès aléatoire (RAM), à une mémoire de programme MM ainsi qu'à une mémoire type de clé MC qui est une mémoire protégée pouvant être une partie de la mémoire MM.

L'unité de traitement est également reliée à un écran d'affichage à cristaux liquides AF ainsi qu'à un clavier Cl comportant par exemple des touches de commande de mouvements dans deux directions orthogonales. Enfin, l'unité de traitement est reliée à une interface de communication-boîtier ESB apte à coopérer avec l'interface de communication ESC, et pouvant par exemple comporter un connecteur mécanique disposé dans un logement dans lequel peut être inséré le connecteur de l'objet portatif. L'interface ESB comporte également des moyens de conversion série/parallèle reliés au bus interne du boîtier.

L'ensemble des moyens de ce boîtier est alimenté par des moyens d'alimentation autonomes AL tels que des piles. Tout ou partie des composants de ce boîtier peuvent être réalisés sous la forme d'un Asic.

La mémoire de travail MT est dimensionnée de façon à pouvoir recevoir l'applicatif de jeu stocké dans la mémoire MJ de l'objet tandis que la mémoire MM contient le programme de gestion interne du boîtier (gestion des entrées/sorties, gestion du clavier, de l'écran, programme de chargement de l'applicatif dans la mémoire de travail...).

Selon l'exemple de réalisation décrit en référence à la figure 3, chaque station de validation ST comporte un bloc de traitement articulé autour d'un processeur PR relié à une interface d'entrée/sortie ESS capable de coopérer avec l'interface d'entrée sortie ESC de l'objet portatif. Par ailleurs, la station est reliée par l'intermédiaire d'une liaison appropriée, à un fichier central TB contenant des informations nécessaires, comme on le verra plus en détail ci-après, à la vérification de l'information de résultat contenue dans l'objet portatif.

Le processeur PR de la station incorpore de façon logicielle les différents moyens fonctionnels nécessaires au fonctionnement de celle-ci (cryptage, décryptage, comparaison, lecture...).

On va maintenant décrire plus en détail, en se référant particulièrement aux figures 4a à 4b, un premier mode de mise en oeuvre du procédé selon l'invention.

Sur un site de fabrication, l'ensemble de données de jeu numériques JE, formant le logiciel applicatif de jeu, est traité par des moyens de traitement comportant un algorithme de calcul de certificat d'authentification du type SHA (Secure Hash Algorithm) bien connu de l'homme du métier. Ce dernier pourra cependant, pour plus de détails, se référer à la publication 180-1 du 31 mai 1994 diffusée par le FIPS (Federal Information Processing Standards).

Ces moyens de calcul déterminent un certificat d'authentification CTF à partir de fonctions logiques opérant sur les bits des données numériques de jeu (étape 1). Ainsi, pour un bloc de 1 kilo octet d'applicatif, le certificat d'authentification comporte par exemple 120 bits.

A partir d'une clé de cryptage-jeu Km, commune à tous les objets portatifs, à tous les boîtiers et à toutes les stations de validation, des moyens de cryptage, par exemple utilisant l'algorithme de cryptage DES (Data Encryption Standard) effectuent un cryptage du certificat d'authentification CTF (étape 2) de façon à délivrer un certificat d'authentification crypté CTFc. Les données numériques de jeu et le certificat d'authentification crypté sont alors stockés dans la mémoire de jeu MJ de l'objet portatif (étape 3).

L'objet portatif est alors prêt à être diffusé dans le public.

Quant au boîtier, on stocke dans la mémoire de clé MC de celui-ci, par exemple lors de sa fabrication sur site, une clé de cryptage-boîtier Kf (étape 4). Le boîtier est alors également prêt à être diffusé dans le public.

Un joueur peut se procurer un tel boîtier auprès d'une station de validation du type de la station ST. Lors de cette opération, on fait coopérer le boîtier et la station par l'intermédiaire d'interfaces de communication respectives de façon à lire (étape 5) la clé de cryptage-boîtier Kf stockée dans la mémoire de clé du boîtier. Ces interfaces peuvent être, notamment quand elles sont du type à couplage capacité/inductif, les mêmes que les interfaces ESB et ESS. Elles

peuvent être également distinctes de ces dernières, par exemple du type mécanique à connecteurs. Le processeur PR de la station de validation connaissant la clé de cryptage-jeu Km, (par exemple stockée dans le fichier central TB) effectue alors par l'intermédiaire de moyens de cryptage du type DES un cryptage (étape 6) de la clé Km à l'aide de la clé de cryptage/boîtier Kf. Cette clé de cryptage-jeu cryptée sous Kf, et référencée Kmc, est alors stockée (étape 7) dans la mémoire de clé du boîtier.

Lorsque le joueur souhaite jouer à un jeu particulier, il se procure auprès d'un détaillant spécialisé un objet portatif contenant le logiciel de jeu correspondant. Le joueur insère alors l'objet portatif dans le logement correspondant du boîtier de façon à faire coopérer les interfaces respectives ESC et ESB de l'objet et du boîtier.

Les moyens de décryptage, par exemple du type DES, incorporés de façon logicielle dans l'unité de traitement UT du boîtier décryptent la clé de cryptage-jeu crypté Kmc. L'unité de traitement lit les données numériques de jeu ainsi que le certificat d'authentification crypté CTFc stockés dans l'objet portatif, par l'intermédiaire d'un protocole série via l'interface ESB. L'unité de traitement UT recalcule alors un certificat d'authentification à partir des données numériques de jeu JE, décrypte le certificat d'authentification crypté CTFc à l'aide de la clé de cryptage-jeu Km, compare le certificat d'authentification recalculé et le certificat d'authentification stocké de façon à vérifier l'authenticité du logiciel de jeu (étape 8).

L'ensemble de données numériques de jeu JE est stocké dans la mémoire de travail MT du boîtier de façon à pouvoir être exploité ultérieurement et directement par l'unité de traitement UT aux fins d'exécution du jeu.

Il convient de noter ici que, notamment lorsqu'on utilise un certificat de type SHA, la vérification de l'authentification du logiciel de jeu JE peut se faire soit "au fil de l'eau", soit lorsque l'ensemble du logiciel a été transféré dans la mémoire de travail MT, cette dernière solution nécessitant une plus grande capacité de mémoire vive.

A ce stade, le boîtier est apte au jeu et le joueur peut jouer à l'aide de son boîtier (étape 9).

A la fin du jeu, ou en cours de celui-ci selon le type de jeu employé ou l'issue de celui-ci, une information de résultat IFR est délivrée par le logiciel de jeu, et celle-ci est cryptée (étape 10) par l'unité de traitement UT en utilisant une clé de cryptage-résultat qui est, dans le cas présent, identique à la clé de cryptage-jeu Km. On obtient alors une information de résultat cryptée IFRc qui est transférée via les interfaces respectives du boîtier et de l'objet portatif de façon à être stockée (étape 11) dans la mémoire de résultat MR de l'objet.

Le joueur peut alors aller faire valider son résultat de façon à toucher éventuellement son gain.

Pour ce faire, le joueur retire l'objet portatif du boîtier, et le communique à une station de validation, qui peut être la même que celle auprès de laquelle il s'est procuré son boîtier, ou bien une autre. On établit alors une coopération entre l'objet portatif et la station. Le processeur PR de la station lit alors dans la mémoire de résultat de l'objet portatif (étape 12) l'information de résultat cryptée IFRc et les moyens de décryptage de cette station, par exemple du type DES, connaissant la clé de cryptage-jeu Km, décryptent l'information IFRc de façon à obtenir l'information de résultat IFR et permettre le paiement du gain.

Si le joueur décide ultérieurement de jouer à nouveau, il lui suffit de se procurer un autre objet portatif contenant un jeu du même type ou d'un type différent et de le faire coopérer avec son boîtier pour jouer.

Dans la variante de mise en oeuvre illustrée sur la figure 5, et destinée à augmenter la sécurité du dispositif, il est prévu une altération 20 du certificat d'authentification crypté CTFc de l'objet portatif après que la vérification de l'authentification du logiciel de jeu a été effectuée par l'unité de traitement du boîtier. Cette altération consiste par exemple en une modification de la valeur de certains au moins des bits du certificat d'authentification.

Par ailleurs, avant de stocker l'information de résultat cryptée IFRc dans la mémoire de résultat de l'objet, on vérifie si cette altération a eu lieu (étape 21). Dans l'affirmative, on autorise le

stockage dans la mémoire de résultat MR et dans la négative, on interdit ce stockage.

D'une façon générale, l'objet portatif est alimenté par l'intermédiaire du boîtier ou de la station. Toutes les fonctions qui viennent d'être décrites en relation avec les données stockées ou à stocker dans l'objet portatif, notamment l'altération du certificat d'authentification, peuvent être effectuées directement de façon logicielle par l'unité de traitement du boîtier. Dans ce cas, le microprocesseur CPU de l'objet portatif peut être omis. Ceci étant, l'existence d'un tel microprocesseur permet d'effectuer ces opérations d'altération (ou d'invalidation) et de vérification d'altération puis d'interdiction éventuelle d'écriture de l'information de résultat cryptée, directement au niveau de l'objet portatif. De même, l'existence d'un microprocesseur CPU sur l'objet portatif permet éventuellement un cryptage du logiciel de jeu au niveau de l'objet portatif avant transfert dans la mémoire de travail du boîtier.

Il se peut également que la clé de cryptage-résultat utilisée pour crypter l'information de résultat ne soit pas la clé de cryptage-jeu Km et ne soit pas connue à l'avance par la station de validation. Il peut en être ainsi lorsque la clé de cryptage-résultat est tout simplement la clé de cryptage-boîtier Kf. Dans ce cas, le mode de mise en oeuvre illustré sur la figure 6 prévoit non seulement le stockage de l'information de résultat cryptée IFRc dans la mémoire de résultat de l'objet (étape 11) mais aussi le stockage, dans cette mémoire de résultat ou dans une autre mémoire (étape 30, d'une information de clé ICR permettant ultérieurement de déterminer la clé de cryptage-résultat qui a été utilisée pour crypter l'information de résultat.

Cette information ICR peut être par exemple la clé de cryptage-résultat proprement dite ou bien un identifiant du boîtier qui est associé de façon biunivoque au boîtier et par conséquent à la clé de cryptage-boîtier Kf qui a été stockée.

Le processeur de la station de validation lit alors (étape 31) l'information de clé ICR et détermine à partir d'une table de correspondance entre les identifiants et les clés de cryptage-boîtier, stockée, de préférence de façon protégée, dans le fichier TB, la clé de

cryptage-résultat Kr (en l'espèce la clé Kf) qui a été utilisée (étape 32).

Il peut être ensuite procédé au décryptage de l'information de résultat (étape 13).

Cette variante de l'invention permet en outre d'identifier précisément les boîtiers ayant conduit à des jeux gagnants et d'effectuer éventuellement des statistiques. Ceci offre une possibilité supplémentaire de détection d'une fraude éventuelle si l'on s'aperçoit qu'un même boîtier conduit très souvent à des jeux gagnants.

REVENDICATIONS

1. Procédé d'activation et de protection anti-fraude d'un dispositif électronique de jeu comportant au moins un boîtier (BT) dans lequel a été stockée au moins une clé de cryptage-résultat, ainsi qu'au moins un objet portatif (OB) capable de coopérer avec le boîtier et dans lequel a été stocké un ensemble de données numériques de jeu authentifiable (JE) et représentatif d'un jeu, procédé dans lequel on fait coopérer l'objet portatif avec le boîtier, on vérifie (8) au sein du boîtier l'authentification de l'ensemble de données de jeu et on stocke cet ensemble de données de jeu dans une mémoire de travail (MT) du boîtier, de façon à autoriser le déroulement (9) du jeu au niveau du boîtier, puis, après le déroulement d'au moins une partie du jeu, on crypte (10) au sein du boîtier une information de résultat (IFR) dépendante dudit jeu à l'aide au moins de ladite clé de cryptage-résultat, et on stocke (11) cette information de résultat cryptée (IFRc) dans une mémoire de résultat (MR) de l'objet portatif, puis, on fait coopérer l'objet portatif avec une station de validation (ST) ayant accès à ladite clé de cryptage-résultat, ladite station effectuant un traitement de validation (13) à partir au moins de ladite information de résultat cryptée et de ladite clé de cryptage-résultat.

2. Procédé selon la revendication 1, caractérisé par le fait que le traitement de validation comporte un décryptage de l'information de résultat cryptée.

3. Procédé selon la revendication 1, caractérisé par le fait qu'on stocke dans l'objet portatif, conjointement avec l'information de résultat cryptée, l'information de résultat non cryptée, et par le fait que le traitement de validation comporte un recryptage de l'information de résultat non cryptée stockée dans l'objet portatif et une comparaison de cette information de résultat recryptée avec l'information de résultat cryptée et stockée dans la mémoire de résultat de l'objet portatif.

4. Procédé selon l'une des revendications 1 à 3, caractérisé par le fait que lorsque l'authentification de l'ensemble de données de

jeu de l'objet portatif a été vérifiée et que ledit ensemble a été stocké dans la mémoire de travail du boîtier, on interdit (20) toute exploitation ultérieure, par le boîtier, de l'ensemble de données de jeu de cet objet portatif.

5. Procédé selon la revendication 4, caractérisé par le fait que, le dispositif comprenant plusieurs boîtiers et plusieurs objets portatifs, lorsque l'authentification de l'ensemble de données de jeu de l'un des objets portatifs a été vérifiée et que ledit ensemble a été stocké dans la mémoire de travail de l'un des boîtiers, on interdit toute exploitation ultérieure, par l'un quelconque des boîtiers, de l'ensemble de données de jeu de cet objet portatif.

6. Procédé selon l'une des revendications précédentes, caractérisé par le fait qu'on authentifie l'ensemble de données de jeu stocké dans l'objet portatif en lui adjoignant un certificat d'authentification (CTF) lié de façon biunivoque audit ensemble de données de jeu (JE) et par le fait que la vérification de l'authentification de l'ensemble de données de jeu comporte un recalcul du certificat d'authentification au sein du boîtier et une comparaison entre le certificat d'authentification recalculé et le certificat d'authentification stocké dans l'objet portatif.

7. Procédé selon la revendication 4 ou 5 prise en combinaison avec la revendication 6, caractérisé par le fait qu'on interdit toute exploitation ultérieure d'un ensemble de données de jeu en altérant, dans l'objet portatif correspondant, au moins partiellement ledit certificat d'authentification et/ou au moins partiellement l'ensemble de données de jeu.

8. Procédé selon l'une des revendications précédentes prise en combinaison avec la revendication 4, caractérisé par le fait qu'on autorise (21) le stockage de l'information de résultat cryptée dans l'objet portatif que si l'on a, au préalable, interdit toute exploitation ultérieure de l'ensemble de données de jeu de cet objet portatif.

9. Procédé selon l'une des revendications précédentes, caractérisé par le fait que l'on stocke dans le boîtier une clé de cryptage-boîtier (Kf).

10. Procédé selon l'une des revendications précédentes,

caractérisé par le fait qu'on stocke dans le boîtier au moins une clé de cryptage-jeu (Km), par le fait que l'authentification de l'ensemble de données de jeu stocké dans l'objet portatif comporte un cryptage au moins partiel de cet ensemble de données de jeu, ou d'une information (CTF) reliée à cet ensemble de données de jeu, à l'aide de la clé de cryptage-jeu (Km), avant lecture par le boîtier, et par le fait que la vérification de l'authentification de cet ensemble de données de jeu comporte un décryptage au sein du boîtier à l'aide de la clé de cryptage-jeu.

11. Procédé selon les revendications 6 et 10, caractérisé par le fait que l'on crypte et on décrypte uniquement le certificat d'authentification (CTF).

12. Procédé selon la revendication 9 prise en combinaison avec la revendication 10 ou 11, caractérisé par le fait que l'on stocke dans le boîtier la clé de cryptage-jeu (Km) ayant été cryptée à l'aide de la clé de cryptage-boîtier (Kf).

13. Procédé selon la revendication 9 prise en combinaison avec l'une des revendications 10 à 12, caractérisé par le fait que, le dispositif comportant plusieurs boîtiers et plusieurs objets portatifs, une clé de cryptage-boîtier (Kf) différente est associée à chaque boîtier tandis que la clé de cryptage-jeu (Km) est commune pour tous les boîtiers et à tous les objets portatifs, par le fait que la clé de cryptage-boîtier d'un boîtier est stockée dans celui-ci avant le stockage de la clé de cryptage-jeu, et par le fait que l'ensemble de données de jeu d'un objet portatif est stocké dans celui-ci, déjà au moins partiellement crypté, ou associé à une information (CTFc) déjà au moins partiellement cryptée, à l'aide la clé de cryptage-jeu.

14. Procédé selon la revendication 9 ou l'une des revendications 10 à 13, caractérisé par le fait que la clé de cryptage-résultat (Kr) est la clé de cryptage-boîtier (Kf), ou la clé de cryptage-jeu (Km), ou est obtenue à partir d'une combinaison de la clé de cryptage-boîtier et de la clé de cryptage-jeu.

15. Procédé selon l'une des revendications précédentes, caractérisé par le fait que l'on stocke dans l'objet portatif coopérant avec le boîtier, une information de clé (ICR) associée de façon

biunivoque à ladite clé de cryptage-résultat, et par le fait que la station de validation a accès à ladite clé de cryptage-résultat en lisant ladite information de clé stockée dans l'objet portatif.

16. Procédé selon l'une des revendications précédentes, caractérisé par le fait que l'ensemble de données de jeu (JE) d'un objet portatif est lu par l'intermédiaire d'un protocole série entre l'objet portatif et le boîtier.

17. Dispositif électronique de jeu, caractérisé par le fait qu'il comprend au moins un boîtier (BT), au moins un objet portatif (OB), et au moins une station de validation (ST), par le fait que l'objet portatif comporte une mémoire de jeu (MJ) contenant un ensemble de données de jeu (JE) authentifiable et représentatif d'un jeu, une mémoire de résultat (MR) apte à contenir une information de résultat cryptée (IFRc), une première interface de communication (ESC) apte à coopérer avec une interface de communication-boîtier (ESB), et une deuxième interface de communication (ESC) apte à communiquer avec une interface de communication-station (ESS), par le fait que le boîtier comporte une mémoire de clé (MC) contenant une clé de cryptage-résultat, une mémoire de travail (MT) accessible en écriture et en lecture, et une unité de traitement (UT) reliée à ces mémoires ainsi qu'à l'interface de communication-boîtier, l'unité de traitement étant capable, lors d'une coopération entre l'interface de communication-boîtier et la première interface de communication de l'objet, de vérifier l'authentification de l'ensemble de données de jeu mémorisé dans l'objet et de stocker ledit ensemble dans la mémoire de travail de façon à permettre le déroulement du jeu au niveau du boîtier, puis de crypter une information de résultat (IFR) dépendante dudit jeu, à l'aide de la clé de cryptage-résultat, et de communiquer cette information de résultat cryptée (IFRc) à l'interface de communication-boîtier aux fins de son stockage dans la mémoire de résultat de l'objet, et par le fait que la station de validation (ST) comporte des moyens (PR) aptes à déterminer ladite clé de cryptage-résultat et des moyens de traitement-station (PR) aptes à lire l'information de résultat cryptée via l'interface de communication-station, lors d'une coopération entre l'objet portatif et la station, et à

effectuer un traitement de validation à partir au moins de cette information de résultat cryptée et de la clé de cryptage-résultat.

18. Dispositif selon la revendication 17, caractérisé par le fait que les moyens de traitement-station comportent des moyens de décryptage-station aptes à décrypter l'information de résultat cryptée.

19. Dispositif selon la revendication 17, caractérisé par le fait que l'unité de traitement du boîtier est apte à communiquer également l'information de résultat non-cryptée à l'interface de communication-boîtier aux fins de son stockage dans la mémoire de résultat de l'objet, et par le fait que les moyens de traitement-station sont en outre aptes à lire l'information de résultat non cryptée via l'interface de communication-station, et comportent des moyens de cryptage-station aptes à crypter ladite information de résultat non cryptée à l'aide de la clé de cryptage-résultat, ainsi que des moyens de comparaison pour comparer l'information de résultat cryptée recalculée avec l'information de résultat cryptée stockée dans la mémoire de résultat de l'objet portatif.

20. Dispositif selon l'une des revendications 17 à 19, caractérisé par le fait que la première interface de communication (SEC) de l'objet portatif est une interface série.

21. Dispositif selon l'une des revendications 17 à 20, caractérisé par le fait que l'ensemble de données de jeu authentifiable est associé à un certificat d'authentification et par le fait que les moyens de vérification de l'authentification de cet ensemble de données de jeu comportent des moyens de calcul de certificat aptes à recalculer ledit certificat d'authentification à partir de l'ensemble de données de jeu, et des moyens de comparaison aptes à comparer le certificat recalculé et le certificat stocké dans la mémoire de jeu de l'objet portatif.

22. Dispositif selon l'une des revendications 17 à 21, caractérisé par le fait qu'il comprend des moyens de cryptage aptes à crypter au moins partiellement l'ensemble de données de jeu authentifiables (JE), ou une information (CTF) reliée à cet ensemble de données de jeu, à partir d'au moins une clé de cryptage-jeu, et par le fait que la mémoire de clé du boîtier est apte à contenir ladite clé de

cryptage-jeu tandis que les moyens de vérification de l'authentification de l'ensemble de données de jeu comportent des moyens de décryptage reliés à la mémoire de clé.

23. Dispositif selon les revendications 21 et 22, caractérisé par le fait que les moyens de cryptage cryptent uniquement le certificat d'authentification (CTF).

24. Dispositif selon la revendication 22 ou 23, caractérisé par le fait que les moyens de cryptage (CPU) sont incorporés à l'objet portatif.

25. Dispositif selon l'une des revendications 22 à 24, caractérisé par le fait que la clé de cryptage-jeu est stockée cryptée et par le fait que l'unité de traitement (UT) du boîtier comporte des moyens de décryptage de cette clé de cryptage-jeu.

26. Dispositif selon l'une des revendications 17 à 25, caractérisé par le fait qu'il comprend des moyens (CPU) d'invalidation de l'ensemble de données de jeu authentifiable d'un objet portatif.

27. Dispositif selon l'une des revendications 17 à 26, caractérisé par le fait qu'il comprend des moyens (CPU) d'interdiction de l'écriture de l'information de résultat cryptée dans la mémoire de résultat de l'objet portatif.

28. Dispositif selon la revendication 26 ou 27, caractérisé par le fait que les moyens d'invalidation (CPU) et/ou les moyens d'interdiction (CPU) sont incorporés dans l'objet portatif.

29. Dispositif selon l'une des revendications 17 à 28, caractérisé par le fait qu'il comprend plusieurs boîtiers, plusieurs objets portatifs et plusieurs stations de validation, l'un quelconque des objets portatifs étant capable de coopérer avec l'un quelconque des boîtiers et avec l'une quelconque des stations de validation.

FIG_1

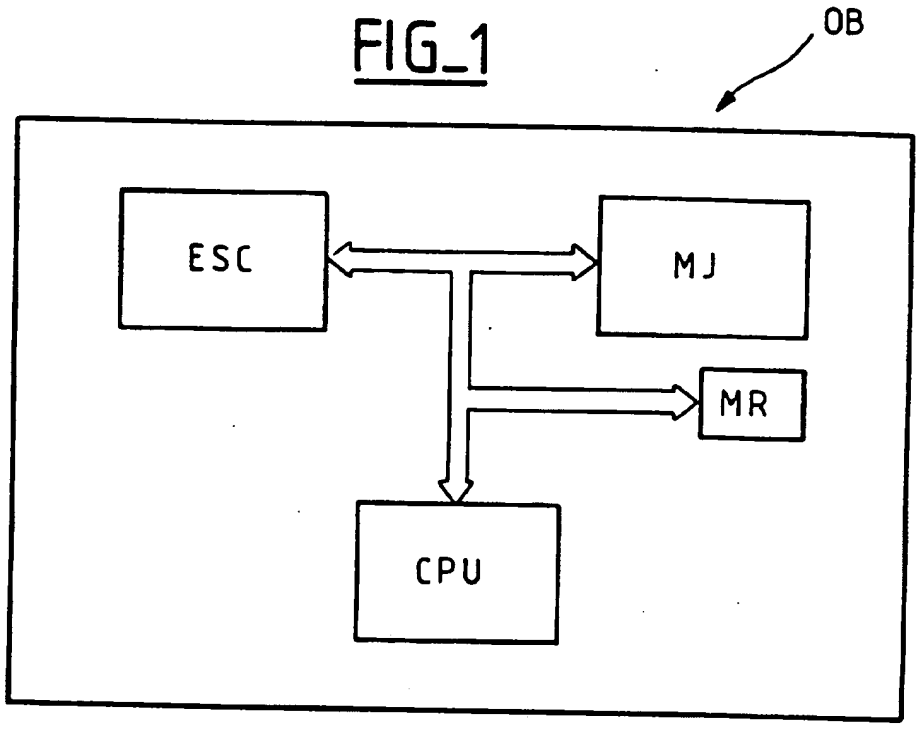


FIG_2

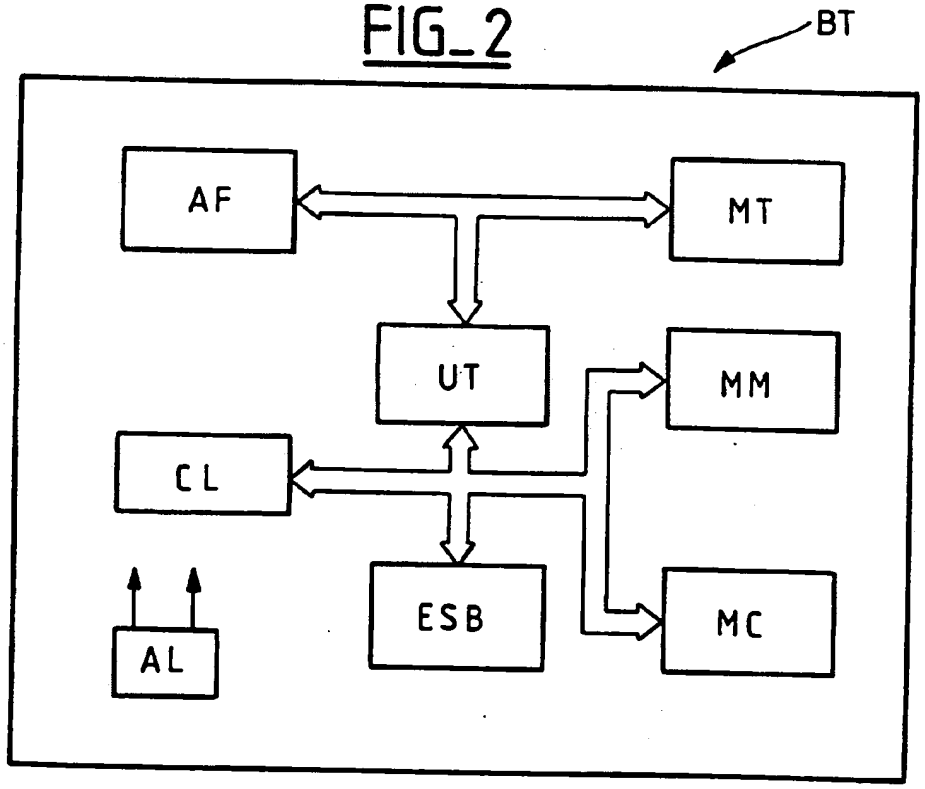


FIG_3

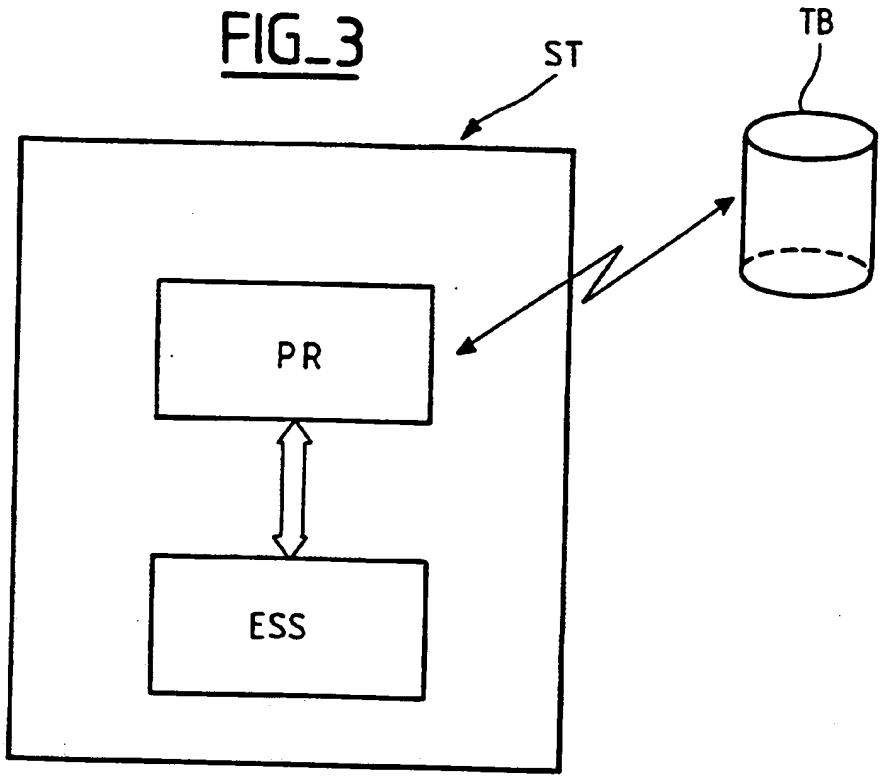


FIG_4a

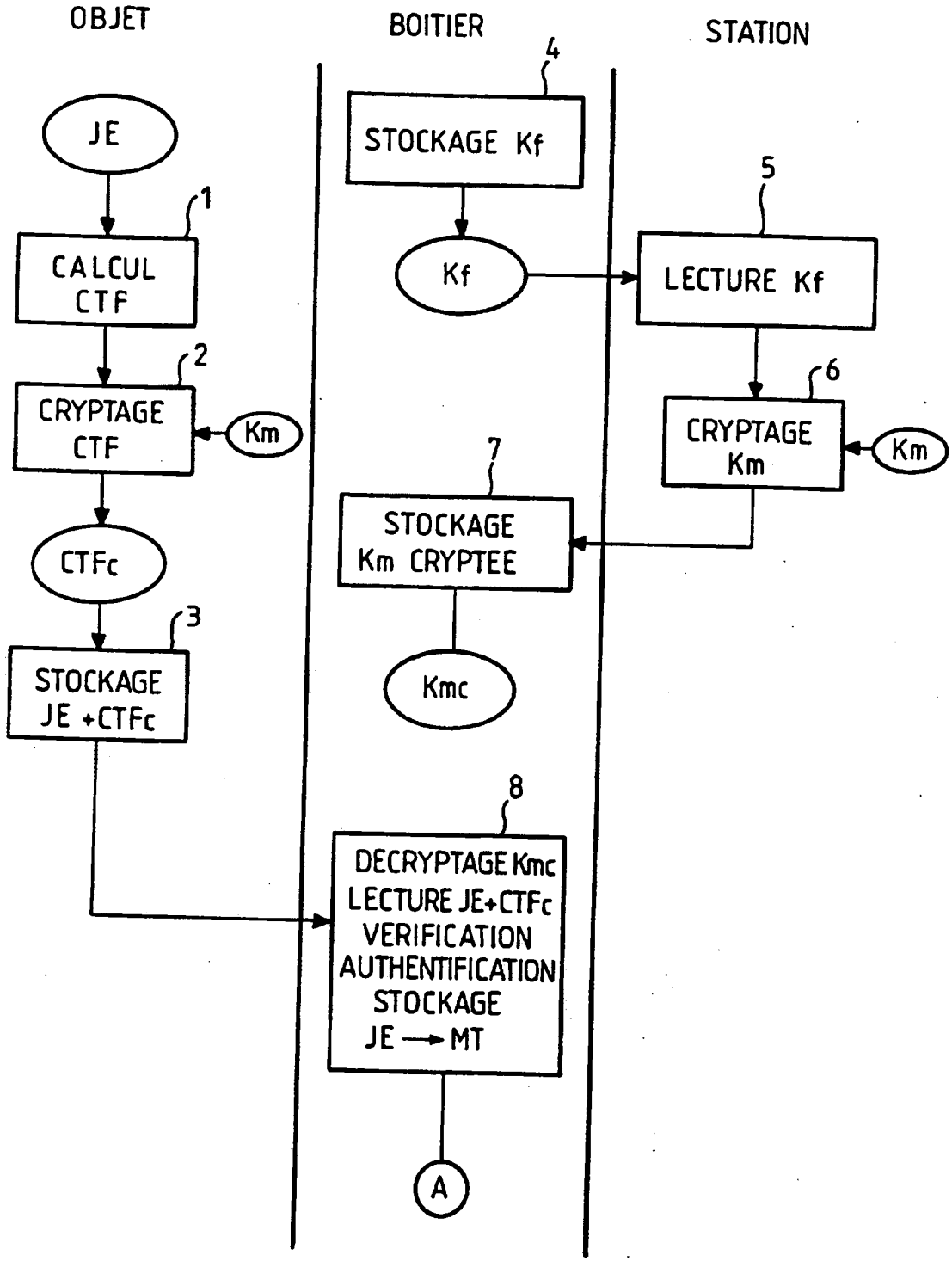

OBJET
BOITIER
STATION
JE
1
CALCUL CTF
2
CRYPTAGE CTF
Km
CTFc
3
STOCKAGE JE +CTFc
4
STOCKAGE Kf
Kf
5
LECTURE Kf
6
CRYPTAGE Km
Km
7
STOCKAGE Km CRYPTEE
Kmc
8
DECRYPTAGE Kmc
LECTURE JE+CTFc
VERIFICATION
AUTHENTIFICATION
STOCKAGE
JE → MT
A

FIG_4b

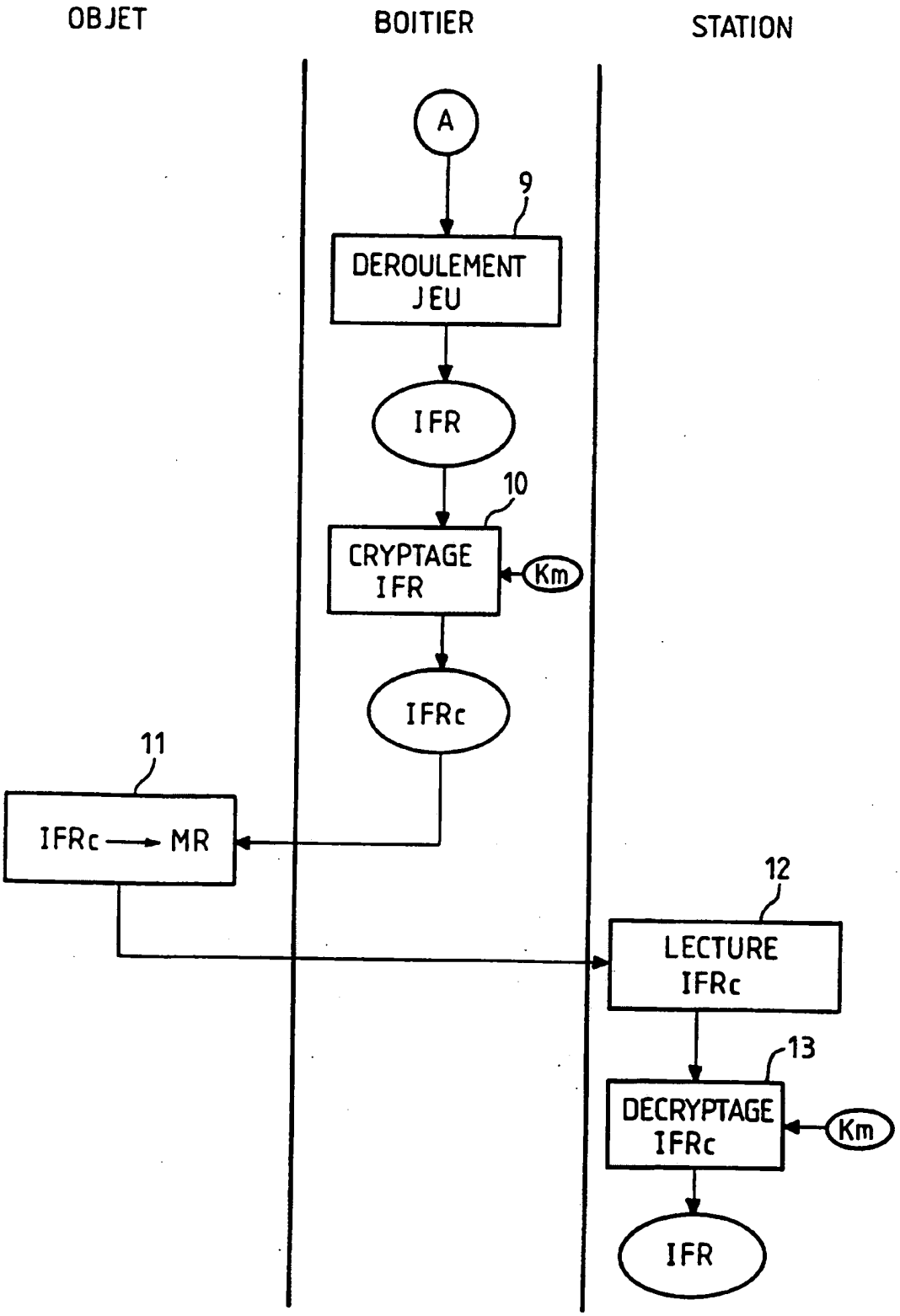

OBJET
BOITIER
STATION
A
9
DEROULEMENT JEU
IFR
10
CRYPTAGE IFR
Km
IFRc
11
IFRc → MR
12
LECTURE IFRc
13
DECRYPTAGE IFRc
Km
IFR

FIG_5

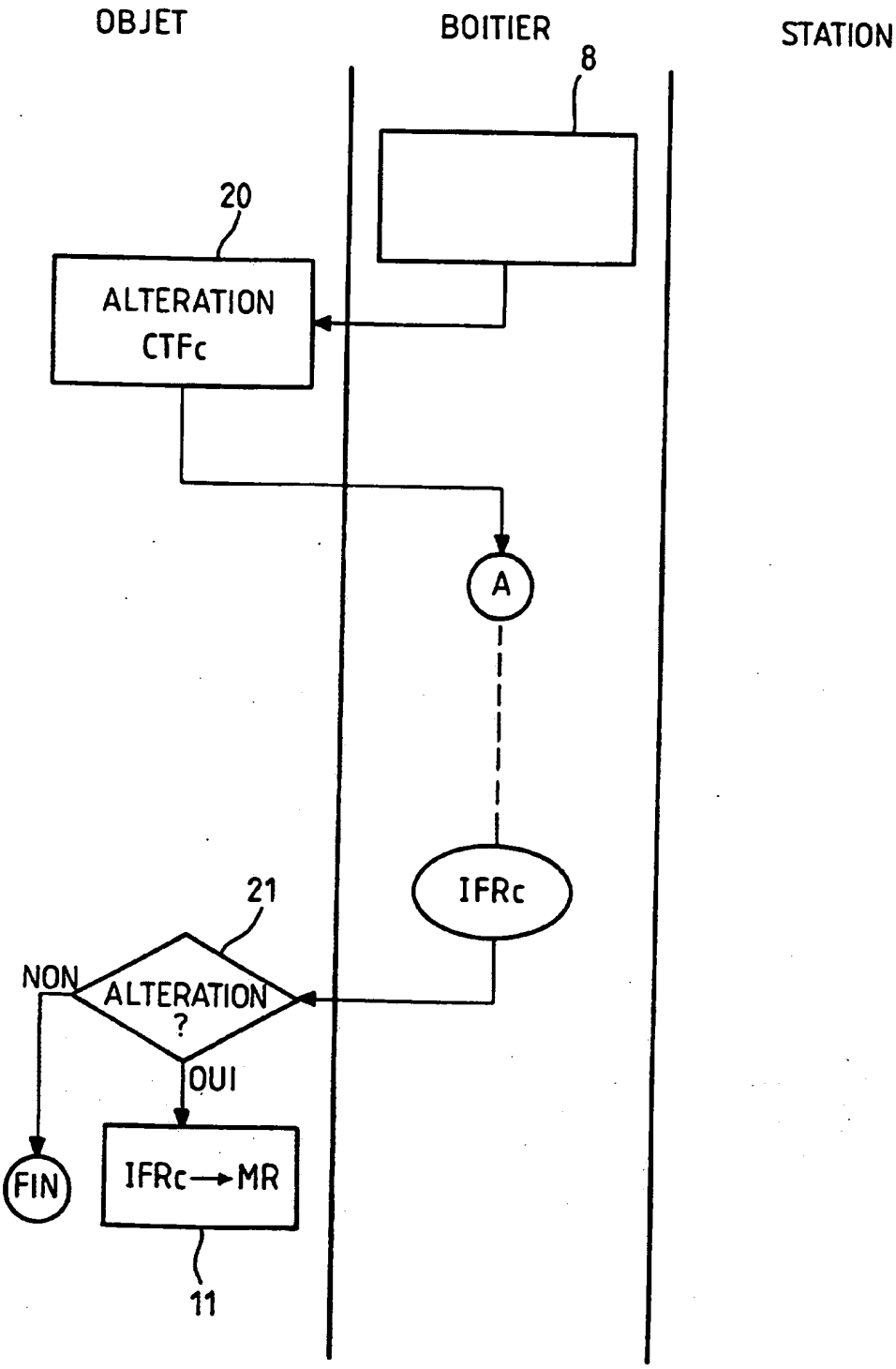
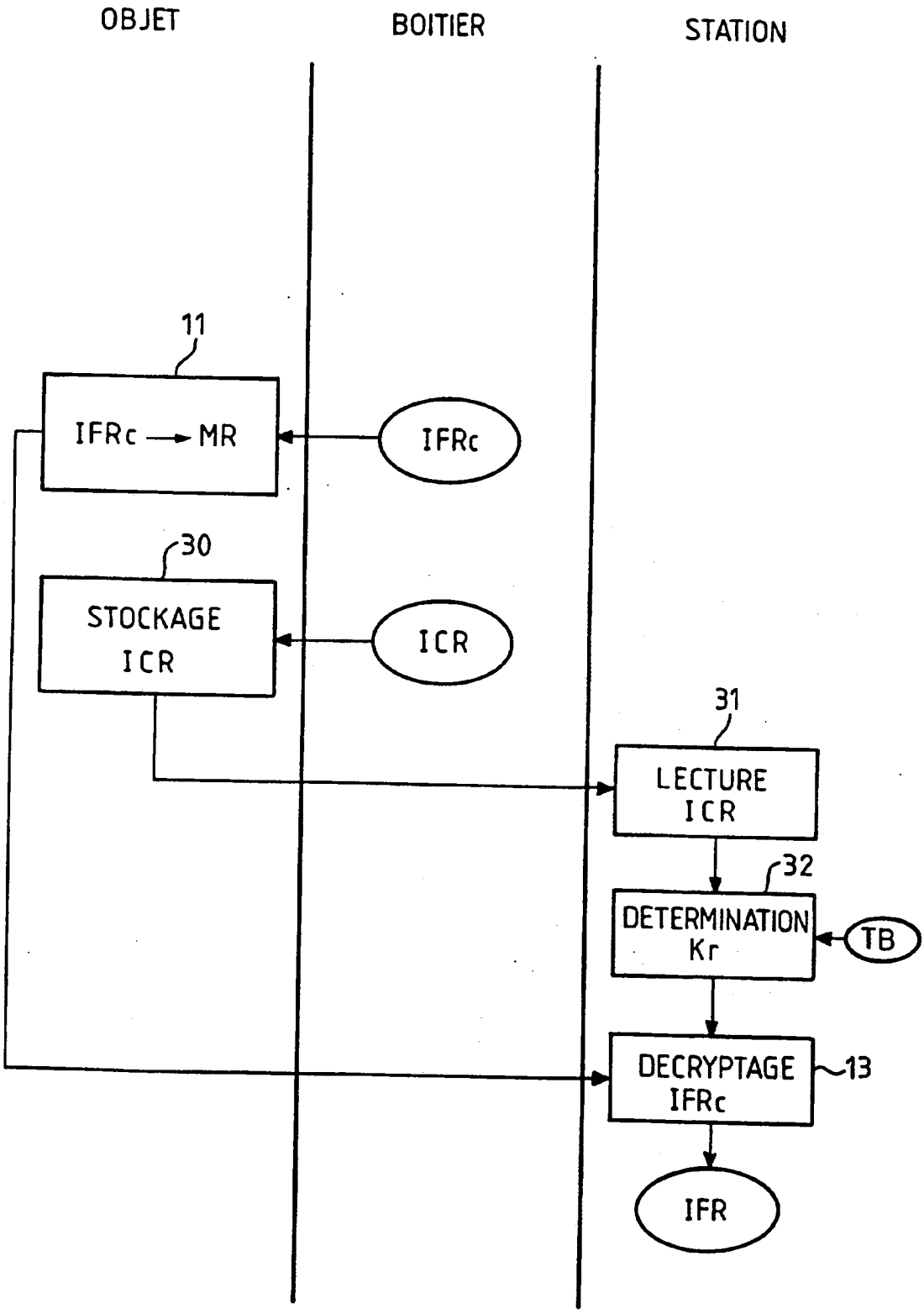

OBJET
BOITIER
STATION
8
20
ALTERATION CTFc
A
IFRc
21
NON
ALTERATION ?
OUI
FIN
IFRc → MR
11

FIG_6


OBJET
BOITIER
STATION
11
IFRc → MR
IFRc
30
STOCKAGE ICR
ICR
31
LECTURE ICR
32
DETERMINATION Kr
TB
DECRYPTAGE IFRc
13
IFR

INTERNATIONAL SEARCH REPORT

Internati Application No
PCT/FR 96/00645

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07C15/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07C G06F G07B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO,A,92 10806 (GTECH CORP) 25 June 1992 see page 1, line 1 - page 11, line 24; figures 1-4	1,17
A	US,A,4 882 473 (BERGERON DANIEL R ET AL) 21 November 1989 see abstract	1,17
A	EP,A,0 547 975 (BULL CP8) 23 June 1993 see abstract see page 2, column 1, line 1 - page 4, column 6, line 18	1,17
A	EP,A,0 360 613 (BALLY MFG CORP) 28 March 1990 see abstract see page 2, column 1, line 1 - page 3, column 3, line 55	1,17

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
27 August 1996	12.09.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer Katerbau, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat Application No
PCT/FR 96/00645

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 462 076 (SMITH III JAY) 24 July 1984 see abstract -----	1,17

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 96/00645

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO-A-9210806	25-06-92	US-A-	5276312	04-01-94
		AU-B-	9153591	08-07-92
		BR-A-	9107145	19-04-94
		OA-A-	9782	15-04-94
US-A-4882473	21-11-89	US-A-	4764666	16-08-88
		AU-B-	2218688	23-03-89
		CA-A-	1294052	07-01-92
		DE-A-	3877868	11-03-93
		EP-A-	0307925	22-03-89
		JP-A-	1222374	05-09-89
EP-A-0547975	23-06-93	FR-A-	2685510	25-06-93
		JP-A-	5274140	22-10-93
		JP-B-	6075251	21-09-94
		US-A-	5253295	12-10-93
EP-A-0360613	28-03-90	US-A-	5179517	12-01-93
		AT-T-	116754	15-01-95
		AU-B-	613484	01-08-91
		AU-B-	3450489	29-03-90
		DE-D-	68920391	16-02-95
		DE-T-	68920391	27-07-95
US-A-4462076	24-07-84	AUCUN		